

## REMARKS

In the Final Office Action mailed August 4, 2005, the Examiner rejected claims 1-10, 12-21, 25-28, and 30-33 under 35 U.S.C. § 103(a) as being obvious in view of *Bisbee* (U.S. Patent No. 6,367,013) in view of *CFSB* (Computer Fraud & Security Bulletin, "How Key Escrow Might Work").

Applicant has amended claims 1, 2, 4, 5, 7, 10, 12, 14-19, 21, 26, 28, and 33 and canceled claims 3, 6, 8, and 20 without prejudice or disclaimer. Claims 1, 2, 4, 5, 7, 9, 10-19, 21, 25-28, and 30-33 remain pending. Based on these amendments and the following remarks, Applicant respectfully traverses the rejection under U.S.C. §103(a).

### **I. The Rejection of Claims 1-33 Under 35 U.S.C. §103(a)**

To establish a prima facie case of obviousness, three basic criteria must be met. First, the prior art reference or references, taken alone or combined, must teach or suggest each and every element recited in the claims. See M.P.E.P. § 2143.03. Second, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to combine the references in a manner resulting in the claimed invention. See M.P.E.P. § 2143. Third, a reasonable expectation of success must exist. See M.P.E.P. § 2143.02. Moreover, each of these requirements must "be found in the prior art, and not based on applicant's disclosure." M.P.E.P. § 2143.

a. The Cited Art Does Not Support the Rejection of Claims 1, 2, 4, 5, 7, 9, 10-19, 21, 25-28, and 30-33

The Examiner asserts *Bisbee* teaches a system that stores information objects and digitally signed, authenticated and encrypted documents or information objects. (Final OA at 3 and 4.) Although the system taught by *Bisbee* does store encrypted information objects, *Bisbee* does not disclose or suggest storing a user's encryption key. Indeed, *Bisbee* states that the information maintained by the system includes documents or objects that have already been signed by keys or other security mechanisms (See e.g., *Bisbee*, col. 8, lines 40-65 and col. 12, lines 30-42.) Accordingly, *Bisbee* does not support the rejections. For example, *Bisbee* does not teach or suggest at least encrypting a user's encryption key with a first archival key and storing the encrypted user's encryption key in a database, as recited in claims 1 and 33.

The Examiner admits *Bisbee* does not teach "providing an indication of proof of storing the encrypted user's encryption key, wherein the indication of proof is signed with a second archival key." (Final OA at 3.) To satisfy this deficiency, the Examiner asserts *CFSB* teaches this feature, citing to portions of the first and fourth paragraphs of *CFSB*. (Final OA at 3.) As explained in the Amendment filed June 17, 2005, neither *CFSB* or *Bisbee et al.* support the Examiner's position for establishing a *prima facie* case of obviousness. The mere fact that *CFSB* describes key certificates signed by a key holder does not provide a showing that the cited art, alone or in combination, teaches or suggests the recitations of the claims. For instance, the Examiner's interpretation that "the key escrow certificate is served as

the indication of proof that the key has been escrowed when provided to CA as taught by *CFSB*,” does not address the claimed recitations that the request is provided to the certificate authority based on the verification of the signed indication of proof, as recited in claims 1, 15, and 33. (Final OA at 3.) That is, according to *CFSB*, the certificate authority (i.e., “CA”) receives proof that a key has been escrowed, and does not address receiving a request from a user for a digital certificate based on the verification of the signed indication of proof, as recited in claims 1, 15, and 33.

Further, the Examiner improperly misconstrues the cited art to support the asserted rejections of Applicant’s claims. For Example, the Examiner asserts the “Registration Manager (RM)” (i.e., RA as noted in *Brisbee*) corresponds to a requesting entity. Based on this premise, the Examiner alleges the “RM” must receive an indication of proof that it can “verify the indication of proof is indeed performed and sent by the authorized key escrow agent certified as meeting the standards.” (Final OA at 4.) To support this assertion, the Examiner refers to a portion of *CFSB*, which merely describes the choice of users in selecting a certified key holder. (See Final OA at 4 and *CFSB*, ¶ 4, lines 1-2.) This portion of *CFSB*, nor any other portion, does not support the Examiner’s conclusion that a “requestor” (i.e., a request for a digital certificate) “must” receive a verification that a key has been escrowed. Indeed, *CFSB* specifically teaches away from such an assertion in stating that the “CA would need proof that the key has been escrowed.” (*CFSB* at ¶ 1, lines 5-6.) Moreover, the cited art, most notably *CFSB*, would not suggest sending the request to a certificate authority based on the verification of a signed indication of

proof because, as noted above, the certificate authority is the entity that receives the “proof” of an escrowed key. Accordingly, the cited art does not support a *prima facie* case of obviousness, as asserted by the Examiner.

Further, the cited art does not teach or suggest the recitations of the pending claims. *Bisbee* discloses a system that includes a certificate authority, a registration authority, and a TCU. The certificate authority implements a repository (DCR) for storing certificates, thus is under control of the certificate authority (See *Fig. 2*). The registration authority may interact with the certificate authority to collect certificates. The TCU, as explained above, stores signed documents or information objects and provides proof of authenticity of these documents for other entities. Contrary to the Examiner’s assertions, none of these elements, or any others disclosed by *Bisbee* suggest a registration manager configured to receive a digital certificate request including a user’s encryption key, send the user’s encryption key, and in response receive an indication of proof of archival. Further, *CFSB* merely describes using an escrow agent to maintain a key and the possible use of escrow certificates, which falls short of describing or suggesting the implementation of a registration manager or similar entity, as recited in the pending claims.

Further, contrary to the Examiner’s assertions, the cited art does not disclose or suggest a data recovery manager or similar entity configured to receive the user’s encryption key, send the user’s encryption key to a database for archiving, create an indication of proof archival, and send the indication of proof of archival, as recited in the pending claims. As explained, the TCU taught by *Bisbee* does not store user encryption keys. Instead, the TCU maintains signed documents and/or information

objects. Further, nowhere does *CFSB* disclose a recovery manager or similar entity as recited in the pending claims. Indeed, the cited art falls short in describing a data recovery manager or similar entity that sends an indication of proof and a registration manager or similar entity that receives the indication of proof. Additionally, the cited art fails to disclose a certificate authority that issues a digital certificate when it is determined that the indication of proof was received. While *CFSB* states a certificate authority would need proof that a key has been escrowed through an escrow certificate, the reference does not disclose a registration manager that receives an indication of proof and a certificate authority that issues a digital certificate when it is determined the indication of proof was received.

Thus, *Brisbee*, alone or in combination with *CSFB*, fail to teach or suggest process steps and/or elements associated with a registration manager, recovery manager, and certificate authority or similar entity, as recited in the pending claims. Instead, as noted above, *CFSB* merely discloses systems that may use a certificate authority and a key holder that provides an escrow certificate and does not disclose processes and elements associated with a registration manager or similar entity that interacts with these entities, as recited in the pending claims. Further, although *Brisbee* describes a system including a certificate repository, a trusted custodial utility, a certificate authority and a registration authority, none of these systems perform processes individually or collectively in a manner similar to the recitations of the pending claims. Nor does either cited reference make up for the deficiencies of each other to suggest the recitations of the pending claims. Contrary to the requirements for showing a *prima facie* case of obviousness, none of the cited art

teaches or suggests these features. Therefore, Applicant respectfully requests the rejection of claims 1, 2, 4, 5, 7, 9, 10-19, 21, 25-28, and 30-33 under 35 U.S.C. § 103(a) be withdrawn and the claims allowed.

Moreover, the Examiner improperly ignores recitations of certain claims in asserting the cited art teaches or suggests Applicant's claims. As such, the Examiner has not met the requirements of M.P.E.P. § 2143 to establish a *prima facie* case of obviousness. For example, the Examiner merely rejects claims 10, 12, 16, 17, 18, 28, and 30 for the "same reasons set forth for claim 1." (Final OA at 7.) These claims, however, recite features that are not claimed in claim 1, and thus require consideration and a showing by the Examiner that the cited art renders the features obvious. The Examiner has not done so in the Final Office Action. Accordingly, should the Examiner maintain these rejections, further explanation of the Examiner's positions in light of the recitations of these claims are requested.

b. There is No Motivation to Combine Cited Art as Asserted by the Examiner

Moreover, *prima facie* obviousness has not been established at least because there is no motivation to combine *Bisbee* and *CFSB*. Determinations of obviousness must be supported by evidence in the record. See *In re Zurko*, 258 F.3d 1379, 1386 (Fed. Cir. 2001) (finding that the factual determinations central to the issue of patentability, including conclusions of obviousness by the Board, must be supported by "substantial evidence"). Further, the desire to combine references must be proved with "substantial evidence" that is a result of a "thorough and searching" factual inquiry. *In re Lee*, 277 F.3d 1338, 1343-1344 (Fed. Cir. 2002) (quoting *McGinley v. Franklin Sports, Inc.*, 262 F.3d 1339, 1351-52).

In this case, the Office Action does not show that a skilled artisan considering *Bisbee* and *CFSB*, and not having the benefit of Applicant's disclosure, would have been motivated to combine or modify the references in a manner resulting in Applicant's claimed combination. In fact, the Examiner merely states a conclusion of the alleged combination without providing the requisite motivation to support the combination. The Examiner alleges that a skilled artisan would have modified *Bisbee* because "CFSB teaches a more flexible and security enhanced method to manage the digital certificate in the sense that users could choose a secure independent 3<sup>rd</sup> party as an key escrow agent (different from the CA) that is certified as meeting the standard to provide a high level of assurance that keys are not compromised or misused." (Final OA at 4.) This conclusion is not properly supported and does not show that a skilled artisan would have modified the reference as alleged. The mere fact that *CFSB* mentions a secured key escrow system does not show that a skilled artisan would have been motivated to modify *Bisbee* as alleged.

The M.P.E.P. makes clear that: "[t]he mere fact that references can be combined or modified does not render the resultant combination obvious unless the prior art also suggests the desirability of the combination" M.P.E.P. § 2143.01 (citations omitted). The Examiner has not shown that the cited art "suggests the desirability" of the alleged combination. Indeed, there is no reason why a skilled artisan would look to modify *Bisbee* with *CFSB*. For example, the TCU taught by *Bisbee* has no need for a key escrow agent because it maintains already signed documented and information objects. Further, the certificate authority itself maintains a repository of certificates (DCR), thus having a key escrow agent for these

certificates is not needed. Therefore the conclusions in the Office Action were not reached based on facts gleaned from the cited references and that, instead, teachings of the present application were improperly used in hindsight to reconstruct the prior art. For at least these additional reasons, the Examiner has not established a *prima facie* case of obviousness with respect to the pending claims, and thus, the rejection of these claims under 35 U.S.C. § 103(a) should be withdrawn and the claims allowed.

## **II. Conclusion**

In view of the foregoing remarks, Applicant submits that this claimed invention, is neither anticipated nor rendered obvious in view of the cited art. Applicant therefore requests the Examiner's reconsideration and reexamination of the application and the timely allowance of the pending claims.


Please grant any extensions of time required to enter this response and charge any additional required fees to our deposit account 06-0916.

Respectfully submitted,

FINNEGAN, HENDERSON, FARABOW,  
GARRETT & DUNNER, L.L.P.

Dated: November 28, 2005

By: \_\_\_\_\_

  
Joseph E. Palys  
Reg. No. 46,508